Annex III

Terms of Reference (TOR)
eDeclarations Information System & Portal

Contents

Introduction

Objectives of the Document

The technical specifications have been developed in the framework of the project „Assistance to the Implementation of e-Governance Component of the National Strategy of Edification of Information Society in the Republic of Moldova". The content of the document is based upon a study of opportunities for the establishing of an Action Plan in the creation and implementation of an Informatics System for the Main State Fiscal Inspectorate. The technical specifications have been discussed by the Technical Advisory Group of the project, with the participation of representatives of the Ministry of Information Development, Main State Fiscal Inspectorate, and Centre of Special Telecommunications.

The objectives of the present document are:

- setting requirements towards the Information System & Portal „e-Declarații (e-Declarations)" of the Main State Fiscal Inspectorate (SI „e – Declarații" (e-Declarations)) regarding the organizational and functional structures, Databases (DB) and informatics applications;
- identification of the information sources for the completion and updating of centralised DB;
- determination of the structure, principles of distribution and volume of information streams;
- determination of the principles to be applied in the establishing of relationships between the beneficiaries and administrators of the System;
- setting up principles of data collection, inserting of data in the Database (DB), and principles of distribution of processing tasks;
- determination of the domain (area) of System functioning and application.

The requirements established in the Document will serve as a basis for the Offer preparation in the framework of the tender aimed to select a company that will elaborate and implement the system.

1. Problem Analysis

1.1 System Definition

The Information System & Portal «eDeclarations»of the Main State Fiscal Inspectorate is intended for the collecting, storing and processing of fiscal reports of taxpayers (physical and juridical persons). The proposed version of the informatics system will follow the basic principles of the e-Governance implementation concept, and will include the components contained in the mentioned concept.

The Informatics System «eDeclarations» constitutes a multitude of methodological and informatics means carrying out functions of creation, administration and consult of Database on the relationships between the Main State Fiscal Inspectorate and "outside" subjects: taxpayers, state superior institutions, other institutions, including the carrying out of the functions:

- completion and administration of a centralised Database at the Main State Fiscal Inspectorate (MSFI);
- reception of data from the subjects of the System, both from those within the Inspectorate and „outside" it, via WAN networks, regarding the activities and payments (contributions) effected;
- consult of the MSFI centralised DB, effected by „outside" subjects;
- continuous information assistance, provided to the MSFI leadership and specialists in their activities;
- development of interfaces of the Information System „e - Declarații" and other existing information systems, necessary for MSFI to carry out its functions;
- creation and administration of an archive;
- creation and administration of an internal archive on the functionality of the System.

1.2 Scope and Objectives of the System

The Informatics System «eDeclarations»is destined for the:

- formation of common information space, adequate for the proposed scopes of MSFI activity, including the carrying out of its relationships with taxpayers;
- development of new information resources, motivated by the MSFI development strategy;
- implementation of e-Governance Concept components.

The direct objectives of the system to be developed are:

- promoting the democratic principles in fiscal activities;
- implication of citizens in the activities of fiscal authorities, within the limits established by the law;
- access to fiscal information of public interest;
- increase of efficacy of fiscal public services;
- creation of adequate conditions to involve persons (taxpayers) in the establishing citizens' relationships with fiscal bodies, via information means of the System;

- development of an optimal Database (DB) structure related to the fiscal bodies' activities, and the taxpayers „behaviour" in their relationships with fiscal bodies;
- reduction of the time while presenting data, and the creation of a level of comfort for taxpayers in carrying out their relationships with fiscal bodies;
- decreasing bureaucracy components in the „taxpayer-fiscal body" relationship;
- reduction of the time of effecting the procedures of accumulation, processing and spreading of data regarding the MSFI subdivisions' activities, including those of:
  - data reception from territorial subdivisions;
  - selection and authentication of data;
  - generation (optional, in conformity with established indices), and issuing of statistical and analytical documents;
  - (optional) informing of MSFI specialists on fiscal activities;
- ensuring of completion, authentication and veracity of data;
- creating possibilities of realization of System interfaces with other informatics systems, either already existing or planned to be further developed and implemented for the fiscal bodies, and with informatics systems „outside" the fiscal bodies.

1.3 Domain of Application

The informatics system "e-Declarations":

- will be developed and implemented in order to be exploited by the Main State Fiscal Inspectorate, including – by its territorial subdivisions, and destined to provide assistance to the leadership and specialists of these units. The system is intended to provide information assistance to specialists and:
- will serve as a means of carrying out „taxpayer – fiscal body" relationships;
- will serve as an information assistance source for superior state institutions;
- will develop interfaces with other informatics systems of MSFI and other „outside" institutions.

The system relates to the information space **„taxpayers ⟸ fiscal body ⟹ other institutions"**.

The system is defined as:

- a closed system – in carrying out of strictly internal functions of the Main State Fiscal Inspectorate and its subordinated subdivisions;
- an open system – in providing services to taxpayers, and dissemination, via Internet networks, of public information related to the activities of fiscal bodies.

The access of the staff of the Main State Fiscal Inspectorate and its subordinated subdivisions to the administered System database shall be varied in accordance with attributed functions.

The access of other beneficiaries to the System DB shall be varied, depending on the obligations of fiscal bodies, to ensure the required complexity of the services provided to these beneficiaries.

2 Opportunity and Premise of System Development

2.1 Organisational Structure of MSFI

The Main State Fiscal Inspectorate (MSFI) is the main body responsible for the activity of the Fiscal System in the Republic of Moldova, being subordinated to the Ministry of Finance.

The organisational structure of the MSFI includes the following levels:

- central (MSFI – Chişinău municipium);
- Chişinău municipium - 6 units (Chişinău municipium, Botanica sector, Buiucani sector, Centrusector, Ciocana sector, Rîşcani sector);
- Bălţi municipium;
- district level - 32 units (Basarabeasca, Dubăsari, Anenii Noi, Briceni, Cahul, Cantemir, Călăraşi, Căuşeni, Cimişlia, Criuleni, Donduşeni, Drochia, Edineţ, Făleşti, Floreşti, Glodeni, Hînceşti, Ialoveni, Leova, Nisporeni, Ocniţa, Orhei, Rezina, Rîşcani, Sîngerei, Soroca, Străşeni, Şoldăneşti, Ştefan Vodă, Taraclia, Teleneşti, Ungheni);
- Găgăuzia autonomous territorial unit - 3 units (Comrat, Ciadir-Lunga, Vulcaneşti);
- common control points - 7 units (Anenii Noi, Căuşeni, Criuleni, Dubăsari, Floreşti, Rezina, Ştefan Vodă);

According to their functions, these subdivisions are divided into:

- administrative-economic subdivisions (annex 4);
- subdivisions controlling;
- taxing and payment monitoring;
- information processing;
- information technologies;

The informatics system of the Main State Fiscal Inspectorate functions within the Information Technologies Department - 20 persons who ensure the services of design, development, implementation, WEB support and technical assistance.

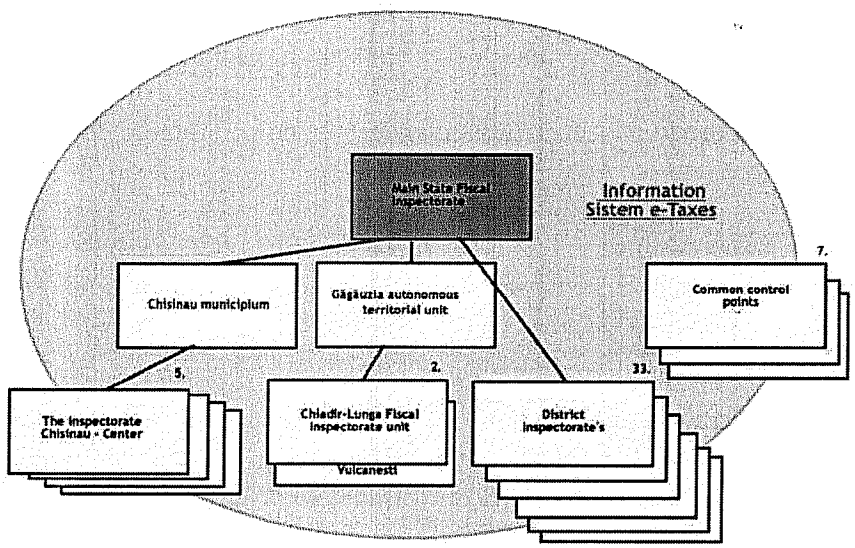

Fig.1 The Organisational System of the Main State Fiscal Inspectorate.

2285 employees are unfolding their professional activities within the Main State Fiscal Inspectorate, out of whom 365 are MSFI employees.

2.2. Description and Assessment of the Existing Informatics System

2.2.1 Technical Equipment Level

The MSFI technical infrastructure, upgraded in the years 2005-2006, includes the following:

- PCs, LAN networks, servers and printers - shared use;
- superior level servers with RISC-processors;
- data storage systems with multiple access (double reliability);
- network equipment for dedicated communications lines (CTS);
- Database Management System (Informix).

Quantitatively, the infrastructure consists of:

- workstations - over 1000 units;
- servers of extended capacity – over 40 units;
- printers – over 670 units.

The arrangement of computerised working places within the Main State Fiscal Inspectorate (MSFI) attains a level of over 51.6%, and namely:

- Main State Fiscal Inspectorate - 69.7%;
- Chişinău municipality Fiscal Inspectorate - 54.2%;
- Bălţi municipality Fiscal Inspectorate - 45.4%;
- Găgăuzia ATU Fiscal Inspectorate - 49,1%.

The operating system for the PCs is Windows 2000 WS or Windows XP. All PCs are part of local networks (LAN) with/or without Internet connection, with connections to electronic email. WEB operative informing service of the MSFI is: www.fisc.md.

2.2.2. Informatization Level, Operational Area of the Existing Systems

The existing MSFI informatics system is a centralised system intended to ensure the collection and procession of all fiscal reports. The methods of organising and processing fiscal documents are contained in the document for internal use „Regulation on the method of centralised organising and processing of document packages" (March, 2004).

As an information unit, the notion of primary document is used. It includes the list of documents presented by the Fiscal Inspectorates on paper support. Document packages are sent to the Main State Fiscal Inspectorate through official post services. The procedures of transmitting, reception and transfer of documents' content to the Database are described in the Regulation. There have been established procedures of quality verification such as the presence of fiscal codes of documents, whose content and form would be in compliance with the data contained in the State Fiscal Register.

The existing informatics system is a functional one and is used by all MSFI subdivisions. But, taking into account the currently existing requirements to informatics

systems, it becomes evident that the existing system can not perform the management of electronic documents, including the data transport via WAN networks.

The Main State Fiscal Inspectorate accepts documents in electronic format from the State Treasury, territorial Treasuries, and National Social Insurance House only. After being processed, all types of received documents are transmitted to the Fiscal Archive. The legislation in force includes a quantity of 166 types of fiscal reports.

Taking as a basis the necessity to undertake the following objectives, established by the Main State Fiscal Inspectorate for the year 2002, and namely:

- document security and accounting.
- usage of advanced equipment and technologies,
- selection of highly qualified specialists,
- development of a republican fiscal archive,
- increase of individual information-processing productivity -

a data-centralised processing system has been implemented.

On the basis of the information contained in the Centralised Database, a set of Reports is created in accordance with the established forms. Certain information of discrete content is transferred to the territorial Fiscal Inspectorates for their administrative fiscal activity. The Centralised Database management uses the following instruments:

- Database creation system - Informix (version10) licensed on processor basis;
- Generation system of DB descriptions - ERWin (version 1.2);
- Database management system - FoxPro;
- System for report issuing - Crystal Reports.

So far, via the existing system, a following estimative number of documents have been processed:

- 3.9 millions documents (2003);
- 5.0 millions documents (2004);
- 5.7 millions documents (2005).

Currently, among the multitude of functions stipulated in the definitions of p. 2 of the present Technical Specifications, a major part of the above mentioned functions are in the process of realization of informatics support, and namely the normative-juridical information assistance to activities of all subdivisions, as well as the functions of collecting in DB the data of documents submitted by taxpayers, the DB management, and generation of resulting documents. So, on the start date of elaboration of Technical Specifications, in the fiscal bodies there functions an autonomous regime included within the local networks.

Each MSFI subdivision, as well as each territorial subdivision is equipped with computers connected to electronic networks (LAN and WAN), but the utilisation of these means does not relate to services provided by the use of the portal „e Taxpayer" and intended to taxpayers .

2.2.3 Functions currently missing in the existing system

In the existing information system are missing some of regular functions and services required by the e-Governance concept. These are:

- Portal functions for public relations with the Main State Fiscal Inspectorate;
- integration functions with the e-Governance Central Portal;
- interconnection services to external information systems (State Registers, Databases, Informatics Systems);

- systems of regular utilization of Internet services;
- security systems of Government Internet communications;
- anti-spy and anti-spam communications protection services;
- digital signature services for data transfer protection and authorization;
- Internet public services for public communication.

The following systematic (continuous) and optional functions are not carried out in the existing system:

- management of a centralised DB (within the leadership of MSFI) that would imply a direct collection of electronic documents from the taxpayers;
- searching, via local network, by the MSFI leadership and specialists, of the centralised DB constituted of generalized data (concerning the activity of the whole fiscal system), and initial data (concerning the activity of concrete subdivision);
- accounting, control and analysis of data concerning the „behaviour" of taxpayers in their relationships with fiscal bodies;
- accounting, quantitative and qualitative analysis of personnel schemes of MSFI territorial subdivisions and leadership;
- Web services integration;
- blog integration;
- integration of consulting forum for persons outside the MSFI;
- utilization of secured electronic mail;
- integration of an anti-spam service .

2.2.4 Evaluations of Existing Information System, Conclusions

The existing information system of the Main State Fiscal Inspectorate can be characterised as a *definite and stable system*, with a potential and possibilities that can be extended to reach *full integration*. The e-Governance concept would contribute to the creation of an effective and righteous system, interoperable with other systems inscribed within this concept.

On the basis of all this, resulting from the objectives established for the Information System „e-Declarații", from the functions partially carried out, as well as those currently not included in the realization process - it can be noted that the existing system:

- has an insufficient methodological and operational support for setting up direct relations „taxpayer $\Longleftrightarrow$ MSFI", using informatics means;
- has a static (indirect) character concerning the setting up of direct relations „taxpayer $\Longleftrightarrow$ MSFI";
- is not adequate to the tendencies of increasing document streams transmitted/received via electronic networks.

On the basis of a succinct analysis and afferent conclusions on the existing situation, we can mention the following:

- the creation of an integrated Information System (IS „e-Declarații") with a complete functional structure, having high performance informatics means as a support, which would function within local networks and WAN networks;

- creation and management, within the foreseen System, of databases supported by all necessary information sources, with a special emphasise of tendencies towards electronic documents;
- granting regular access of users to the database of the System, depending on the strict necessities in the performing of attributed functions;
- granting access of taxpayers to the database of the System, depending on their obligations and on the interest of fiscal bodies to stimulate the carrying out of these obligations;
- informational assistance to superior state bodies, depending on their normative-juridical relationships with fiscal bodies;
- development of interfaces within the integrated Information System „e-Declarații" and other information systems, which are necessary to MSFI in the carrying out of its functions.

Additional premises for the elaboration and implementation of the Portal Integrated Information System „e-Declarații" are:

- presence of a technical-operational support (computers, local electronic networks, Database operational and management systems, etc.), due to availability of significant financial investments;
- availability, within MSFI and its territorial subdivisions, of a sufficient minimum of specialists-users of informatics means, whose knowledge is concentrated on the performing of routine procedures;

3. Requirements to the System

3.1 General Requirements

The scope and objectives imposed by the e-Governanace Concept determine the Information System „e-Declarații" to be:

- adequate to the solutions and requirements of the e-Governance Concept;
- created with its own critical orientation towards user and provided public services;
- scalable – to grant extension capacities, depending on concrete requirements (number of transactions, data volume, number of users);
- interoperable – to grant interconnection, data integration, Internet services, metadata content management with collateral systems;
- standardized – on the basis of respective European Union and the Republic of Moldova standards;
- informationally assured by the market of new information technologies.

In order to reach the scope and objectives, the Information System „e-Declarații" must:

- fully carry out the functional structure in accordance with the project solutions;
- ensure the continuity of the existing information system, at the date of its implementation (IS „e-Declarații") with the view of accepting the MSFI and its territorial subdivisions' organizational structure;
- benefit from structural and functional independency, using the following information sources:
  - internal (own) documents, including normative – juridical documents;
  - documents on electronic support on other types of support, from other institutions or from taxpayers.
- benefit from structural independency, viewed through the possibility of updating (development) one module without affecting others;
- observe information technology standards;
- assure the use of licensed software systems, in order to observe intellectual property rights;
- allow – to foresee the implementation of open software systems, having the right to certify the utilisation of these within the system;
- assure copyright protection of new components, developed within the system;
- benefit from the right to implement digital signature for protection and authorization of data circulation;
- assure flexibility for a permanent adapting to the juridical norms, and with a view to assuring their development after implementation;
- assure data circulation via local networks, and via large-scale application networks, depending on the established regulation;
- have an intelligent user friendly interface;
- be oriented at providing services to an increased number of consult requirements from the users, including those characterised by reduced time intervals, and the simultaneous ones;
- recognise established information sources which „feed" it;
- assure a high level of reliability in exploitation;

- correspond to the requested requirements to information security;
- support the interfaces „user", „beneficiary" and „other systems" in the Romanian language, by using ANSI-latin 1 characters.

3.2 Organisational Structure of the System

The Information System & Portal „e-Declarații" must:

- have a Portal providing taxpayers access to public services;
- have a Gateway capable to authenticate users and secure transactions;
- support the functioning of the e-Governance information system, including eGovernance Portal;
- assure interoperability of data access;
- use licensed software systems, to observe intellectual property rights
- accept implementation of open software systems, having the right to certify their utilisation within the system;
- assure copyright protection of new components elaborated within the system;
- benefit from implementation of digital signature, for the protection of data circulation.

The information system „e-Declarații" supports users who will be, via a portal, offered coordinated, reliable, secured, controlled and protected services. The portal infrastructure –offers persons, in a role of users, a unique, personalised access to information systems. The portal increases the efficiency of business processes, including clients, suppliers, partners and employees.

The user access to the System is assured through the following technical means:

- interactive window, PDA computers, digital television;
- smart card transaction terminals;
- PCs with Internet connection;
- conference-video systems, via IP;
- fax, telephone , mobile telephone, SMS services;
- VoIP systems (digital conversations via IP data specifications).

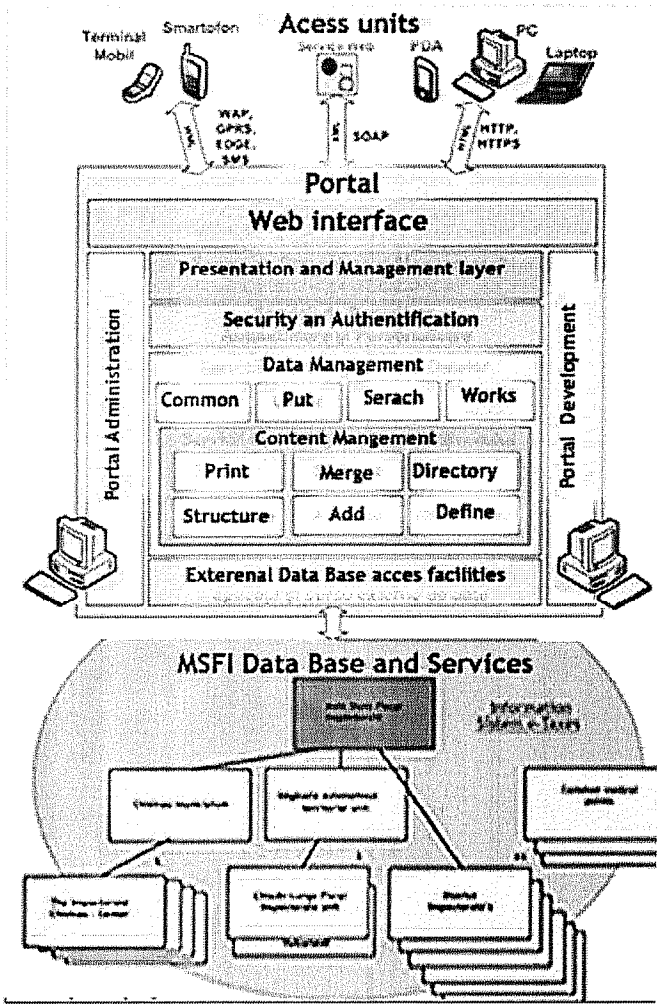

Fig.2 Graphical presentation of the Information System & Portal „e-Declarații".

The portal „e-Declarații" is a component part of the system and, via Web Browser software means, assures the management of direct (on-line) user access to Internet/Intranet.

The portal „e-Declarații" includes a set of applications destined to provide for the user:

- informative ensuring - assistance, training, informing ;
- presence lists - contacts, reference addresses;
- options of system interaction;

The portal "eDeclarații" functionally shall ensure:

- accounting and adapting of users and profiles;
- access security and authentication;
- content management;
- instruments for creating forms of document presentation;
- message mechanisms, routing documents to the addressee, converting them into destinations system format;
- a unitary regulation mechanism, establishing the rules of processing documents;
- working interface;
- content management application;
- a unitary structure for service development, management and maintenance;

as well as to:

- promote a dynamic and efficient communication ;
- include real time instruments of cooperation;
- allow access to business systems;
- assure the management of non-structured information;
- allow the analysis and distribution of business critical information;
- offer services for data management and grant data management.

The gateway is a component part of the system destined to grant a reliable and secure access to data (information), processing the data (information), both via applications of the System „e-Declarații" and via applications of information systems collateral to the e-Governance integrated system. The gateway represents technical resources and software allowing the interconnection of the existing information systems, and granting the access to these via the Internet.

The Gateway system architecture must contain the following basic components:

- Web sites and department portals;
- authentication and registration of users (Registration & Enrolment – R&E);
- transaction management (Transaction Engine – TxE) and document routing;
- integration and regulation mechanisms, via SOAP and UDDI;
- interface servers of departments (Departmental Interface Server – DIS);
- secure message routing system (XML documents).

By using the Gateway, the following benefits shall be granted:

- interaction with public services;
- security and protection of access to data;
- generalised method of XML data presentation;
- description of the method of data transformation from DB;
- assurance of assistance, training, informing;
- provision of personalising options of interaction;
- role and profile management services;
- security and protection against Internet threats;

A preferable version, based on the priorities, advantages and risks of the System functioning, shall be approved in the process of Action Plan elaboration.

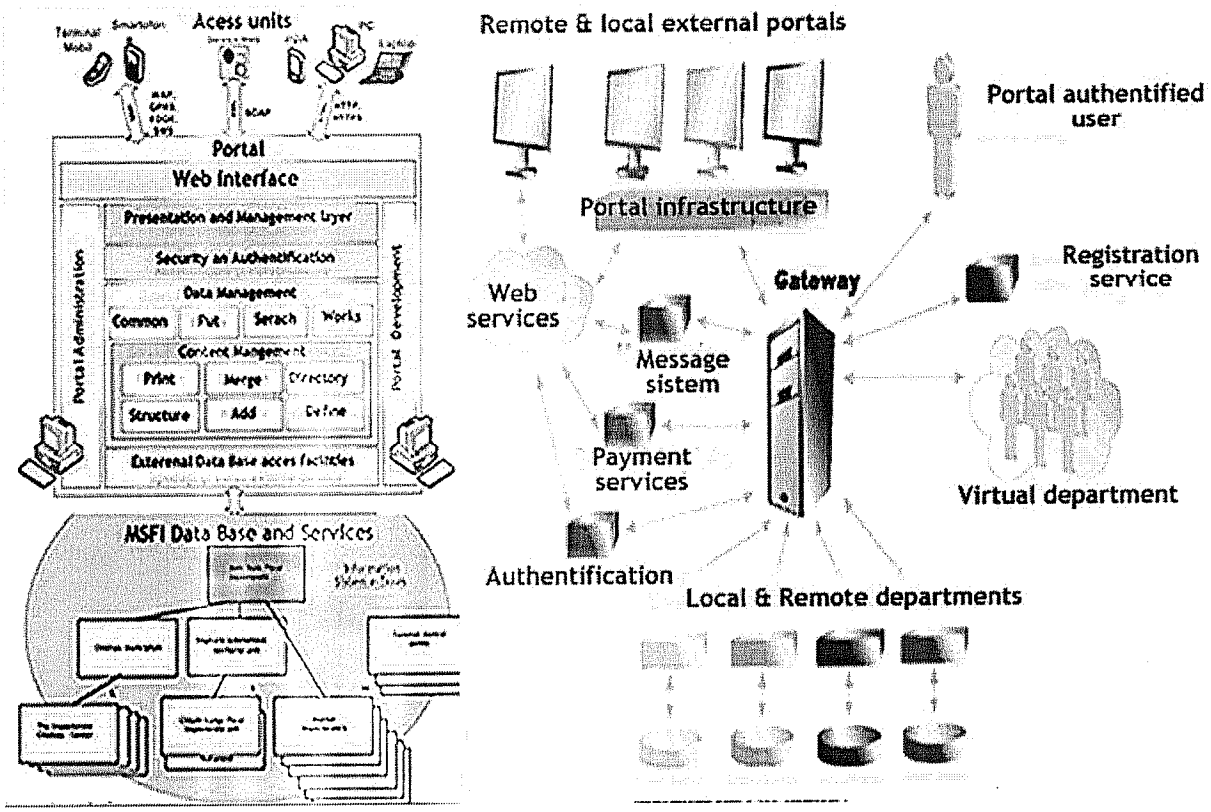

Fig. 3. Graphical presentation of the Information System & Portal „e-Declarații".

3.3 Functional Structure of the System

Proceed from the fact that the System „e-Declarații" automatizes the procedures concerning the relationships „fiscal body – taxpayer" - its functional structures must be of the type „**Client** ⟺ Server ⟺ **Client**".

This type of functional structure provides the centralisation of fiscal administration functions, meaning the creation of a centralised DB at the MSFI central office. This means that the subdivisions' activities of establishing relationships „**server** ⟺ **taxpayer**" are reduced, due to the fact of centralising these activities by the MSFI leadership. The functional structure must be the following:

No. crt.	Section IS „e – Declarații"	Level of performing	Function of the section
1	2	3	4
I	**Providing services to physical and juridical persons („Taxpayer")**	**Server, Central Database**	Reception and rounding up of reports (statistical reports)
			Accounting and analysis of taxpayers' „behaviour" concerning the „reports" compartment
			Completion and issuance, at taxpayer requirement, of data related to the existence of debts/lack of debts
			Creation and management of a library of reporting forms „Formulare"
			Warnings (announcements) for taxpayers exposed on the portal, concerning the non-adequate „behaviour": reports, payments (in case the taxpayer accesses the portal)
			Verification of veracity of data contained in the reports presented by taxpayers, and the respective informing of taxpayers
		Portal (Taxpayer)	Taxpayers identification (by appeals to State Registers- RSP and RSUD)
			Accessing statistics: (non)authorized – DB compartments
			Select menu blocks
			Select menu block procedures
			Select formulation, search the respective consulting instructions
			Document completion
			Launch documents, reception of confirmation from the MSFI, and their inclusion in DB
			Retrieval from DB of previously stored (presented) documents, and their consulting with the relevant mentions. Confirmation of performed procedures
			Retrieval from DB of data concerning own (taxpayer) „behaviour" concerning the „reports" compartment, for desired periods of time
			Warnings (announcements) for taxpayers on portal, concerning the non-adequate „behaviour": reports, payments (when taxpayer accesses the portal)
II.	**Fiscal Administration**	**Workstations installed within territorial subdivisions, which collaborate , via WAN networks, with the MSFI central server**	Multitude of functions, attributed to territorial subdivisions and to concrete specialists within these subdivisions
III	**Management of organisational structure elements of MSFI (MSFI**	32	Institution (company) management informatics systems (for ex.: IS „Document management", „Human resources", „Legislation",

Figure 4 presents a use case diagram, versions of "e-Taxpayer" Portal use

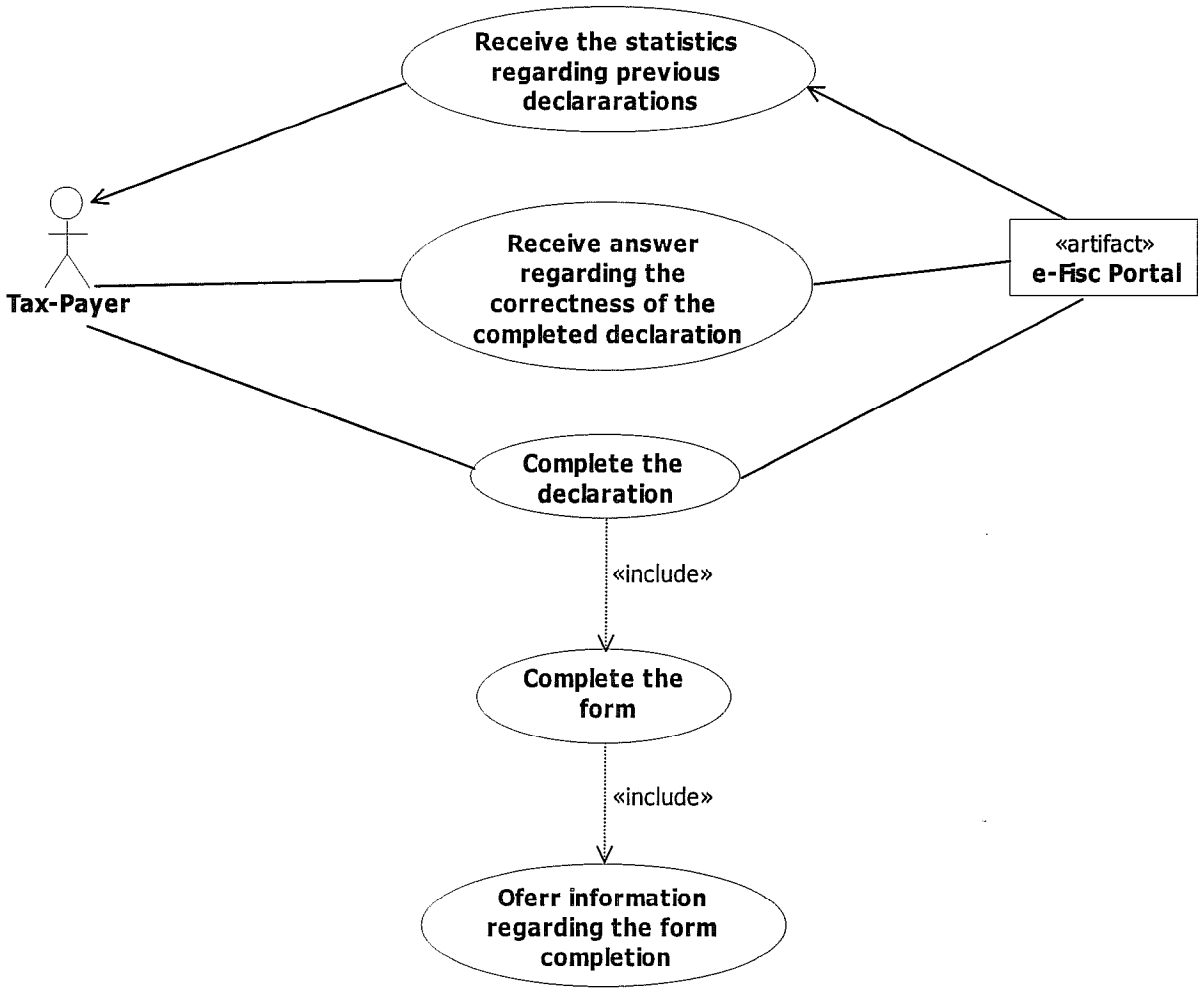

Fig.4. Use Case Diagram. Completion of declaration using the Portal System

Figure 5 represents a scenario of online declaration completion. In this case, a Web page is available; taxpayers can find all necessary types of declarations.

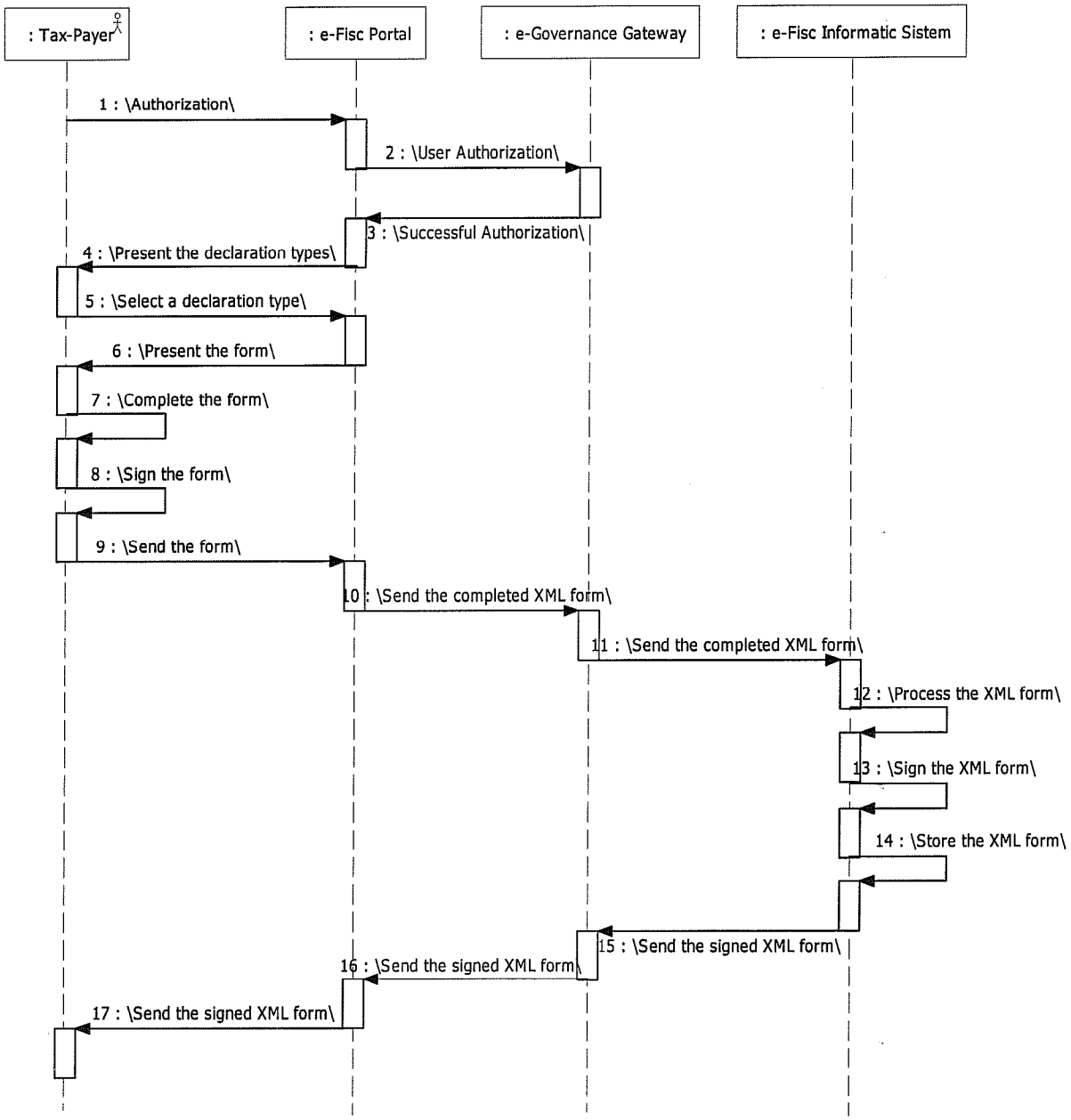

Fig.5. Sequence diagram. Completion of declaration on the portal" e-Taxpayer"

Fig. 6 presents the scenario of loading an already completed declaration. In this case the declaration will be automatically completed, utilizing the XML Scheme language that has been prior downloaded from the portal "e-Taxpayer" .

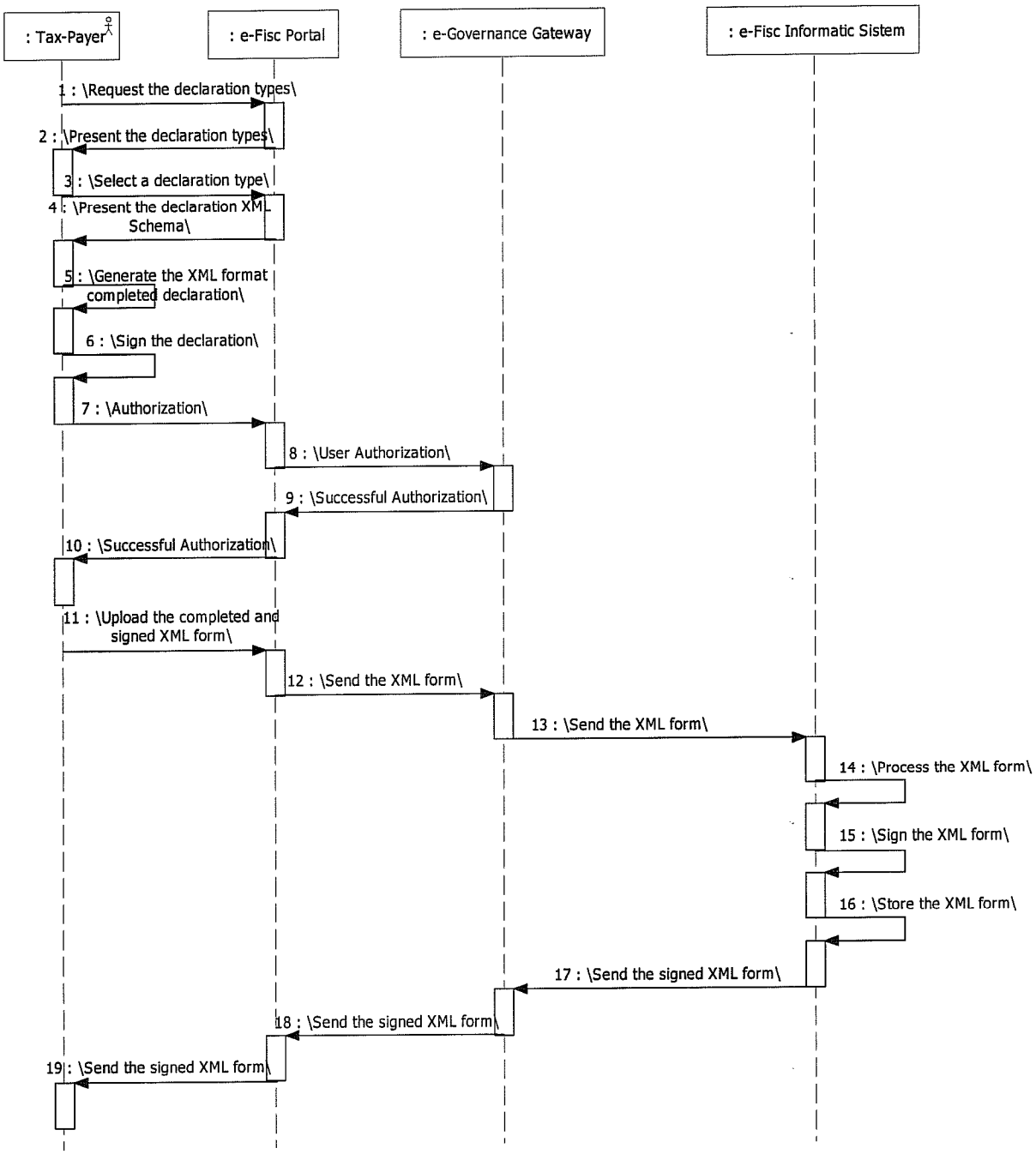
: Tax-Payer
: e-Fisc Portal
: e-Governance Gateway
: e-Fisc Informatic Sistem
1 : \Request the declaration types\
2 : \Present the declaration types\
3 : \Select a declaration type\
4 : \Present the declaration XML Schema\
5 : \Generate the XML format completed declaration\
6 : \Sign the declaration\
7 : \Authorization\
8 : \User Authorization\
9 : \Successful Authorization\
10 : \Successful Authorization\
11 : \Upload the completed and signed XML form\
12 : \Send the XML form\
13 : \Send the XML form\
14 : \Process the XML form\
15 : \Sign the XML form\
16 : \Store the XML form\
17 : \Send the signed XML form\
18 : \Send the signed XML form\
19 : \Send the signed XML form\

Fig.6. Sequence Diagram. Generation of declaration and its loading via the portal "e-Taxpayer"

Fig. 7 illustrates the process of presenting a declaration in the case when the MSFI completes the declaration using fiscal information received from juridical persons. In this case, the taxpayer receives the declaration in XML format. If the form did not suffer modifications, it is signed and loaded via the portal. But, when modifications are needed, these are instilled, after which the taxpayer signs the modified declaration and loads it via the portal.

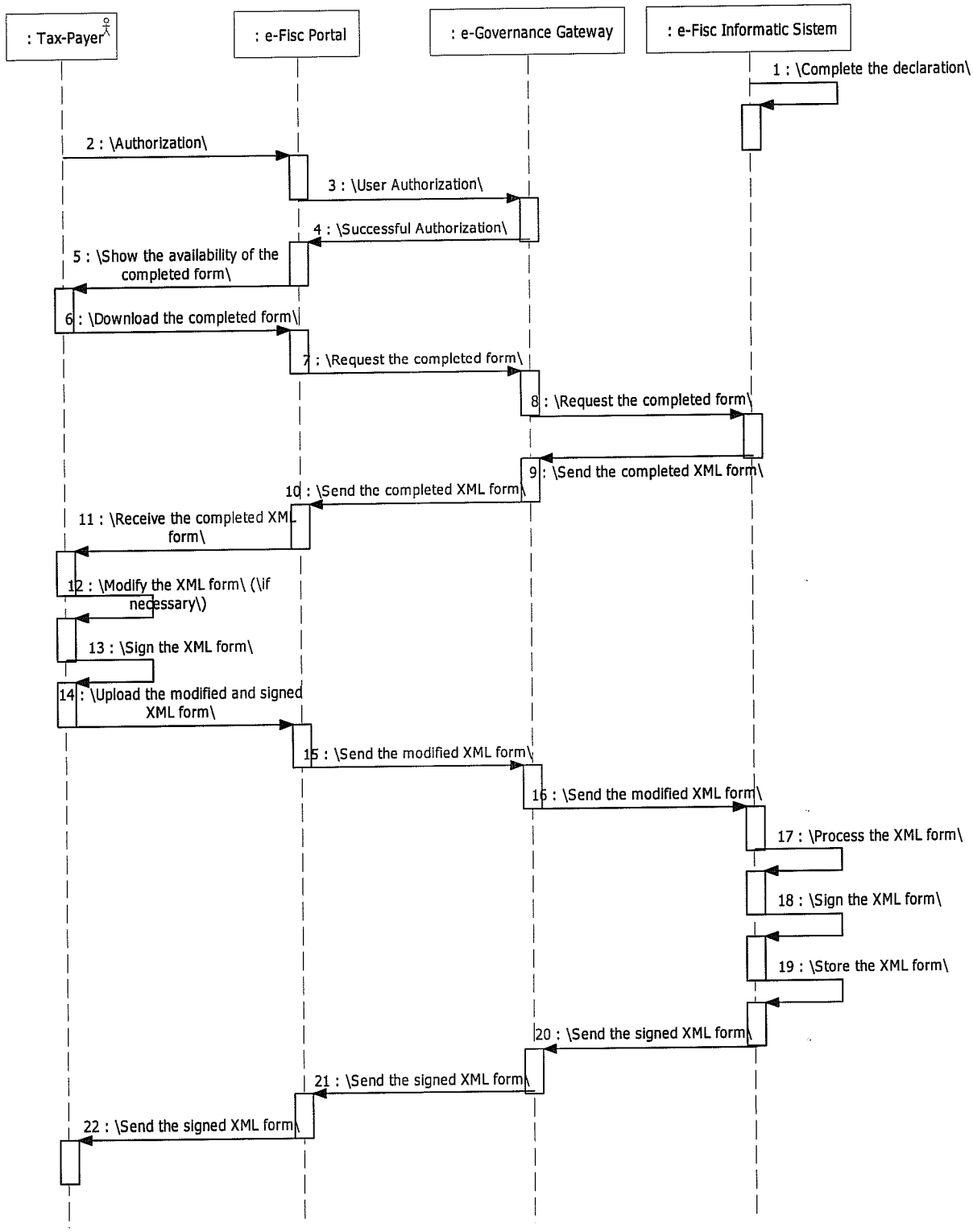

Fig.7. Sequence diagram. Downloading, modification and loading via the portal " e-Taxpayer"

3.4 Database

The requirements towards the Database include:

- creation, according to the functional structure, of primary and resulting documents, established (set up) in the framework of the System;
- compatibility with the existing DB, as well as with the possible modifications in the development of the System;
- ensuring the necessary level of data and DB management software;
- receptivity in the performing of procedures of correcting (modification) of data;
- granting quick access to users with the purpose of data storage, modification, retrieving and consulting;
- DB should be of relational type;
- DB schema – normalized to at least the Normal Form No. 3;
- the use of OLAP technology, or other similar technologies, with the view of gaining online analyses of the data contained in DB;
- Final users' and applications developers' access to data only via SQL queries;
- addition, modification and erasing of DB data is performed only by users authorized with respective functions;
- creation of mechanisms discovering frauds and non-authorised access to data;
- DB must support „multi-user" regime;
- DB working performance must grant a time interval of 5 seconds between queries and reception of results;
- protection of transactions against data loss (committed and rolled back);
- informing the users of successful or unsuccessful transactions;
- DB server must not have any connections with WAN networks;
- DB server management in LAN network will use SSLv3 or VPN;
- support the functions of data backup and data recovery.

3.5 Application Programming Systems

Software set has to assure:

- performing System functions of Database creation and management;
- performing functions of services provided to users via LAN or WAN electronic networks;
- realization of the concept of DB protection and regulation of users access to the data.

The applicative software will contain means of protection against their non-authorised use.

The following software components will be used:

- means for professional development of systems;
- collection and reporting applications;
- monitoring and statistics applications;
- persons 'access applications;
- data analysis and maintenance of the system.

In the programming of system's applications, the emphasis is put on:

- accuracy;
- avoiding double meaning;
- complexity;
- consistency;

- options of importance or stability;
- veracity;
- modifiability;
- traceability.

The software components will be finally established on the basis of the project solutions related to the system functional structure, DB structure and volume (in dynamics), and the project solutions related to the system of data security and protection.

3.6 Technical System of Data Processing and Data Transport

3.6.1 Internet / Intranet Interconnection Systems

The selected Internet or Intranet interconnection specifications are the following:

- alignment to Internet by adopting WWW for the public sector;
- adoption of the XML as a primary standard for data integration and presentation in the public sector;
- Web browser solution to user interface;
- metadata schema for e-Governance information resources;
- Internet protocol IP v4, with options of ulterior IP v6 transition. ;
- message standards SMTP/MIME for the reading of messages, by using POP3;
- standard for secured S/MIME v3. messages;
- SOAP, UDDI and WDSL standards for Web services;
- DNS name resolution services to the Internet and Intranet;
- FTP services with restart and recovery facilities, for large volume files transfer.

3.6.2 Additional Data Transport Systems.

The technical base of the Information System «eDeclarations» consists of personal computers (PCs), including thematic services, printing means, local area networks (LAN) and wide area networks (WAN).

The minimal computer configuration will be determined by the operating system, the volume of applicative software and database volume, exactly established during the stages of System design and realization process.

The integrated system will be installed on the server of the MSFI local networks. Assistance information systems of IS „e-Declarations" for the users within MSFI and its subordinated subdivisions, will be carried out via a web-browser.

The system must:

- be optimal, in the limits of objective norms of depreciation, for the realization of the System functional structure and the ulterior extension of the System;
- contain components existing on the internal market of the Republic of Moldova;
- be of a performance commeasurable with the performance of operating and programming systems;
- be flexible in the utilization of available means destined for reception of information from external resources (other public institutions);
- ensure a high security level of data applications and data transport.

3.6.3 Data Security

Information security must be ensured via a complex system of juridical-normative, organizational and economical measures, by using technological means, software-hardware devices and cryptographic methods of information protection, oriented towards the ensuring of a necessary level of integrity, confidentiality and accessibility of information resources.

Information security must satisfy the following basic requirements:

- complexity;
- concentration for a specific (certain) scope;
- non-interruption;
- reliability;
- centralised management

Threats to information security:

- objects of information security threats are information resources and information infrastructure;
- sources of information security threats can be delinquents, corrupt state functionaries as well as ill-intentioned users;
- the basic threats to information security are:
  - illegal collection and illegal utilization of the information;
  - information processing technology breakdown;
  - implementation in the software and hardware products of components, which carry out unforeseen, unintended functions in the documents accompanying these products;
  - creation and spreading of software affecting the normal functioning of information systems, telecommunications information networks, information protection systems and other informatized systems;
  - erasing, deterioration, radio-electronic suppressing or destruction of processing information means and systems, telecommunication systems and communication systems;
  - influence of automatized systems of information processing and transmission over the protection means;
  - compromising the information protection cryptographic keys and means; - retrieval of information through technical channels;
  - illegal installation of electronic devices, for the purpose of information interception, in technical devices for processing, storing and transmission of information via communication channels, or in offices of state functionaries, with the purpose of information interception;
  - erasing, deterioration, destruction or retrieval of mechanic or electronic information supports;
  - interception of information in data transmission networks and communications lines, decoding of this information and imposing of false information;
  - use of non-certified information technologies, information protection means, means of informatization, telecommunications and communications in the creation and development of information infrastructure;
  - non-authorised access to information resources contained in data banks and databases;
  - violation of the legal restrictions on information spreading;
  - attack against an insufficiently strong key/algorithm;
  - traffic analysis;
  - non-authorised access to workstation;
  - non-authorised access to the network /network resources;
  - covert channels;
  - network spoofing;
  - viruses;
  - spam;
  - tunnelling;
  - Denial of Service (DoS) attack;
  - repudiation;

- the information security threats affect:
  - information confidentiality;
  - logical and physical integrity of information;
  - normal functioning of information infrastructure;
- Information security threats can be realized in the following ways:
  - non-authorised, illegal or non-sanctioned access to information resources and infrastructure;
  - physical influence on the information infrastructure components;
  - illegal information leaking through various channels;
  - bribing and/or threatening the MSFI staff.

The information security system must obligatory include concrete consecutive stages:

- determination of protection profiles;
- categorisation of protected resources;
- risk analysis;
- development of security policy;
- development of security architecture;
- creation and implementation of information security system;
- system certification;
- staff training regarding the methods and procedures of counteracting the threats to information security.

The information security system must be periodically re-examined and readjusted in juridical, organizational, technological and economical aspects. The use of mechanisms ensuring information security must be planned during the design or update stages of information systems, information resources and infrastructure.

The information security system must compulsory include the following basic components:

- information and maintenance of infrastructure protection in case of external networks connection;
- information protection in the process of network interaction;
- data stream protection;
- protection of system services;
- ensuring data integrity;
- antivirus protection;
- anti-spam protection;
- ensuring software security;
- user authentication;
- audit.

The security system must:

- ensure authorized user access to DB, via LAN or WAN networks, using variousof data processing and data consulting procedures, depending on the attributions and obligations of every user;
- include a differentiated system of identification beneficiaries and users, depending on the roles of these in the realization of the System functions;
- allow the identification of taxpayers and other physical and juridical persons, by using The State Registers;

- be receptive to possible modifications in the users' list and/or in the provided to users rights to perform procedures of data processing (inscribing, correcting, erasing, consulting, etc.);
- be receptive to possible modifications of users rights concerning the structural elements of the accessible to them DB;
- include means of creation of back-up copies, on various technical supports;
- include data protection means in cases such as: system deteriorations, non-authorized access, technical accidents;
- include software system security means;
- include data security means at the process of data transport via LAN or WAN networks;
- include means of creation and consult a special data archive concerning the non-authorized access (intentions) to data, indifferently of the stage of data processing or data transfer.

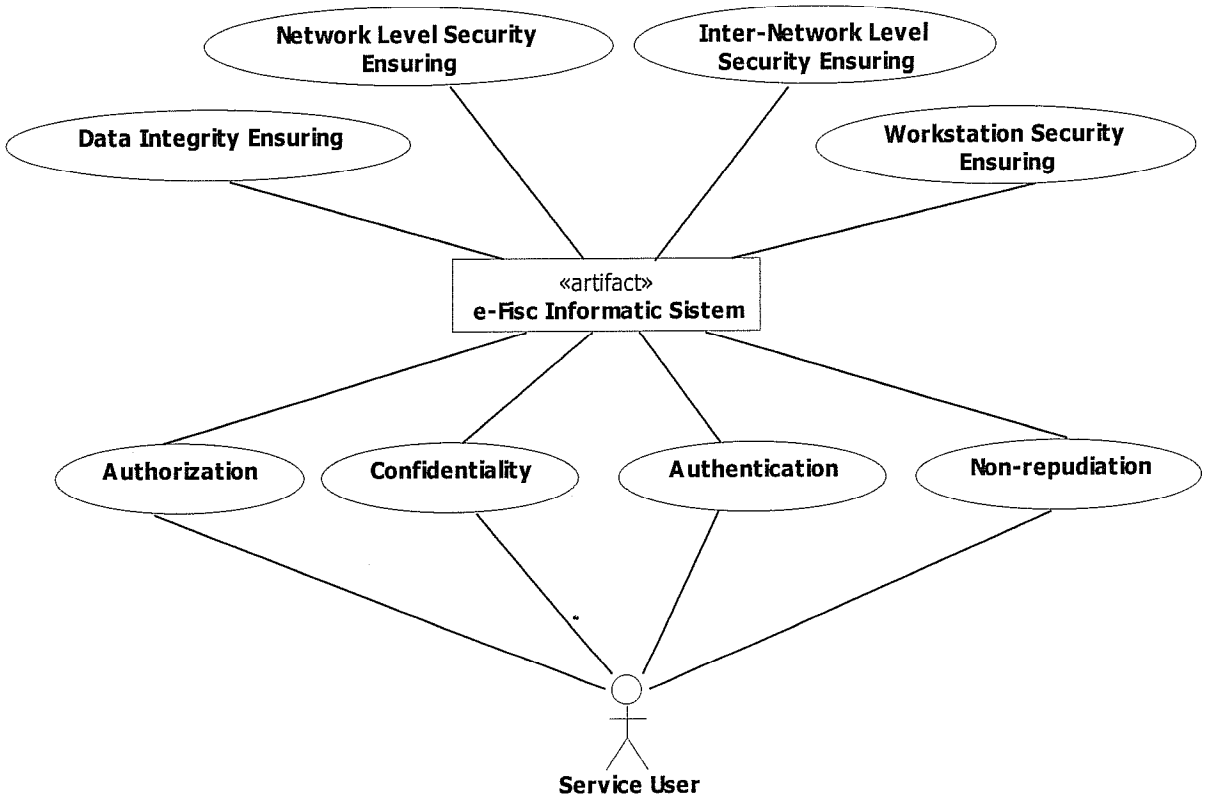

Fig.8 Security of users receiving services provided by MSFI

Information types:

- closed (information that requires high degree of security, personal data, etc.)
- information that requires a medium degree of security
- public (does not require cryptographic mechanisms)
- depending of information importance, there will be selected more strict or less strict protection mechanisms to ensure information protection.

General security:

- MSFI reserves the right to carry out periodical audits of its application infrastructure, in order to ensure compliance with required security standards ;
- In case a damage in the security is identified, the system must have the possibility to effect a partial or total functionality disconnection.

Network security:

- logs must be created for all attempts of access, both successful and unsuccessful ones;
- the MSFI network must be separated from networks of other enterprises;
- the traffic between the database server and the workstations must be encrypted;
- the resources control must be centralised and conform to a well-defined policy;
- access to both hardware and software resources must be divided, depending on user competences

Inter-network security level:

- the network must be protected from external network through a firewall, and the traffic between the security provider and the MSFI will be protected and authenticated through cryptographic technologies;
- Session and state control: the server must preserve the session information when passing information from one page to another (for ex., to avoid a repeated authentication when opening a new page);
- authorised traffic can only enter the system when it is accepted by the imposed security policy;
- the whole traffic passing into and out of the system, must be controlled by the system.

VPN security requirements:

- utilization of VPN will be controlled through authentication, using temporary passwords, such as, for example, token devices or a public/private key system;
- dual tunnelling should not be used. Only one network connection is permitted at a certain given moment;
- VPN users, who do not perform any activity during 20 minutes or more, will be automatically disconnected. At reconnection, the user shall supply authentication information again. Ping or other artificial processes ensuring connection maintenance, shall not be used;
- the connection will have a duration of no more than 24 hours.

Workstation security:

- the computer should be ensured with all the existing at that certain given moment patches for the operating system;
- information should be available regarding the patch installation time;
- administrators must periodically scan workstations, in order to identify vulnerabilities;
- a document regulating the minimum length, the rules of password generation and password validity period should be available;

- local accounts' name/password can not be used for the creation of new external accounts. (in order not to uncover the passwords to third parties);
- there should exist a policy of creation, maintenance and destruction of accounts;
- a selected anti-virus standard package will be used;
- update the anti-virus database.

Standards utilized for elements of public key infrastructure:

- public key certificate formats: X509v3 (RFC2459);
- ensure the possibility of obtaining certificates by utilization of:
  - network protocols: IKE, LDAPv3(RFC 3377);
  - external support: in the format PKCS#7 or PKCS#11-compatible token;
- certificates validity will not have a duration exceeding 12 months;
- the authentication of users will be ensured using a PKCS#11-compatibletoken;
- CRL (Certificate Revocation Lists) and OCSP (Online Certificate Status Protocol) support;
- ensure the reception of revoked certificates in CRL format, utilizing LDAPv3;
- ensure the support S/MIME (Secure / Multipurpose Internet Mail Extensions);
- ensure the SCEP (Simple Certificate Enrolment Protocol) support.

Web-Server:

- authentication (client and server):
  - will be performed on the basis of server and client certificates, in conformity with RFC 2069 Digest Access Authentication;
  - a service of setting the list of trustful certificates should exist;
  - access elements will be changed every 6-12 months;
- application authentication:
  - will be effected at web-server application level;
  - will contain a mechanism of password creation, which will be difficult to identify by means of cryptanalysis;
  - passwords transferred through the network will take the form of hash codes;
- SSL session should be established for all the queries of the client to Web resource;
- data should be kept in a location, other than executable files;
- the server should contain reserve mechanisms for backup and recovery;
- web-server must be installed on a platform separated from other servers;
- the placement of information database on the MSFI work process, and the web-server on same platform is not permitted;
- web-server management will be set using the command prompt;
- web-server management will be effected by a remote terminal, via LAN network, using the command prompt;
- web-server management will be effected by a remote terminal, via WAN network, using the command prompt and VPN tunnelling;
- key change will be effected using the IKE protocol.

Cryptographic modules:

- only standard algorithms (3DES, AES, RSA) should be used for encryption;
- in case of closed information protection, the symmetric key-cryptosystems must have a length ensuring a protection similar to 256-bit AES-key, or 168-bit 3DES-key;
- in case of protection of information requiring a medium degree of security, the symmetric key-cryptosystems must have a length ensuring a protection similar to 128-bit AES-key, or 128-bit 3DES-key;
- in case of closed information protection, the asymmetric key-cryptosystems must have a length ensuring a protection similar to 2048-RSA-key ;
- in case of protection of information requiring a medium degree of security, the asymmetric key-cryptosystems must have a length ensuring a protection similar to 1024-bit RSA-key;
- cryptographic modules should comply with FIPS PUB 140-2 (Requirements for Cryptographic Modules), the concrete requirements must be set during the design stage;
- cryptographic modules should comply with „Approved Key Establishment Techniques for FIPS PUB 140-2";
- cryptographic modules should comply with „Approved Protection Profiles for FIPS PUB 140-2";
- cryptographic modules should comply with „Approved Random Number Generators for FIPS PUB 140-2";
- cryptographic modules should comply with „Approved Security Functions for FIPS PUB 140-2";
- the used hash-functions will be SHA, SHA-256, SHA-384;
- cryptographic modules implementing SHA, should comply with „FIPS PUB 180-2 Secure Hash Standard";
- key algorithms and key length will be annually updated to comply with the technology level of that concrete period of time;
- algorithms will be selected to be utilized only in case they have been approved at international level, being defined as stable and resistant to attack.

Requirements for account database (user names and passwords):

- database user names and passwords should be kept separated from software codes. Access to this database should be offered only to authorized persons;
- accreditation messages (credentials) will be kept on an authentication server (LDAP server used for the authentication of users);

Passwords:

- all system-level passwords (ex.: root password, NT administrator password, administrator account password) should be changed at least once every 3 months;
- all system–level passwords must be administered globally, in a password database;
- all user-level passwords (ex.: email, Web, workstation passwords) should be changed at least once every 6 months. The recommended password validity period equals to a 4-month term;
- the account of the user with privileges at system level, offered to him due to his belonging to a certain group, or through programs of „sudo" (super user do) type, should have passwords different from other accounts of same user;

- passwords SHOULD NOT be inserted in email messages or in other forms of electronic communication;
- in no case the MSFI staff members has the right to share the login and the password with anyone, even with their families.

Remote access:

- the remote access must be strictly controlled. Connection shall be established only with authorised users;
- persons with remote connection to the network must not have other connections at that concrete moment of time. A simultaneous connection with a different network is permitted only when the user is sure of his security;
- routers for ISDN dedicated lines, configured for access to MSFI network , should carry out minimal authorization requirements of CHAP (Challenge Handshake Authentication Protocol);
- organisations or persons who want to utilise a non-standard solution of remote access, must obtain the approval of the administrator.

Physical security:

- the equipment should be placed in a protected location, accessible only to authorised staff;
- the equipment should be placed in a location protected against electromagnetic waves;
- MSFI has the power to authorise persons with the right of access to the equipment.

3.7 System Functioning Statistics

During the whole period of the system functioning, it is necessary to foresee data and processes of functioning monitoring that would make possible the assessment of functionality and the effecting of certain ulterior updating measures.
The monitoring shall be ensured through the following registration of:

- processes;
- messages and the informing mode;
- interventions;
- events and states (situations).

Monitoring data will be appreciated through informative reports and messages, destined to elucidate the situation or the state of system functioning.

The register should contain:

- user identifier;
- date, hour and details of key events (ex.: entry-exit registration system);
- identification of the terminal of access;
- registration of unsuccessful or successful attempts of access to the system;
- registration of changes of system configuration (ex.: changes or attempts of changes of security system settings);

- registration of utilization of privileged accounts (ex.: utilization of supervisor account, root account, administrator account);
- registration of utilization of applications;
- registration of accessed files and access modes;
- registration of network address and protocol address;
- alerts generated by access control system;
- registration of activation and deactivation of protection systems (ex.: anti-virus systems, intrusion prevention/detection systems);
- system alerts (ex.: exceptions to system, exceptions to registration system, alerts concerning network management);
- registration of critical process.

3.8 System Interoperability with other Information Systems (Database), including the State Registers

Insurance of interoperability of the Information System „e-Declarații (e-Declarations)" is an objective destined to ensure a *complete and correct* system functioning. E-Governance concept offers a certain number of solutions, and *organizational*, *technological* and *methodological* modalities for solving this problem. As a final task for the obtaining of the mentioned objective, certain system components should be elaborated.

The *organizational* modality provides a way of organising components. For example, the user authentication is effected through a discrete component (Gateway) of e-Declarations system. The component will secure and ensure the operating in the e-Governance local system and collateral systems.

The *technological* modality provides, in this case, utilization of a single way of XML data representation for the whole e-Governance system.

The *methodological* modality consists, in this case, of the implementation of Internet connection through common security procedures, through forms of user card identification, and digital data presentation form such as, for example, multimedia.

In the component design process, the following recommendations will be taken into account:

- technical platform – Gateway technical solution;
- software platform – operational systems and Microsoft applications;
- technological framework – Internet services with security options;
- special technical requirements – transaction management, user authentication and registration, data security (ISO17999);
- work procedures – State Fiscal Inspectorate, Ministry of Information Development and SIS;
- standardizing - Internet IPv4(RFC), Data security (ISO);
- special options – multilingualism.

The interaction modality between the information systems of State Registers (RSP, RSUD and others), Database (Central Treasury and Territorial Treasuries), National Insurance House and other collateral systems will be established similarly to the Action Plan.

3.9 Special Requirements towards the „Behaviour" of the System with the Taxpayers and Services Provided to These

An objective of great priority for the System „e-Declarații (e-Declarations)" is efficient user access to the system, the mentioned access imposing various *organizational*, *technological* and *methodological* modalities of solving problems. The basic form of the public access to the system is the declaration, notification and performing the tax payments by natural or legal persons who have fiscal obligations to the state. The end task for the attaining of the mentioned objective is finalising the components.

The *organizational* measures review the division of the system in discrete components such as:

- Portal component – ensures the first step of access;
- Gateway component – ensures transactions with collateral systems.

The *technical* measures review the combination of technical solutions such as:

- access security - option provided by the system;
- data presentation – option provided by different solutions at different levels.

The *methodological* measures impose the selection of certain forms of behaviour, depending on user (profile) such as:

- transparency in operating - does not request any knowledge about the solution method;
- dynamic portal infrastructure - eGovernance solution;
- solution excellence - creates a psychological image that predisposes the user to the selected solution.

The *design* measures provide the creation of a system that permits a continuous adapting to the provided means:

- development of access - the possibility to add new technical means;
- access scalability – adapting the technical performance to the existing necessities.

System measures contain measures included in the stage of solution integration, they permit:

- data security – ensured for each component;
- Portal interoperability – ensured through implementation of XML data specifications and eGovernance Interoperability Framework Requirements eGIF.

In the portal design process, the following recommendations will be taken into account:

- technical platform- portal technical solution;
- software platform- operational systems and Microsoft applications;
- technological framework – Internet services with security options;
- special technical requirements – multiple communication channels, duplication of function of some components, flexibility and extensibility for communication sessions;
- work procedures - State Fiscal Inspectorate, Ministry of Information Development and Information and Security Service (ISS);

- informing modality – public information mean;
- standardizing - Internet IPv4(RFC), Data security (ISO);
- special options - multilingualism.

User interface should be functionally complete, commoditised and extensible. The interface should be capable of minimising user errors.

Requirements:

- the content should be included and correctly reflected in a page of 640x480 resolution;
- pages should be dynamically re-dimensioned in order to efficiently use larger browser windows;
- pages must not overload their own fonts to the detriment of the user fonts. The user should have the possibility to adjust the font and its size through standard browser setting;
- all pages must be completely loaded (including the graphics) in 5 seconds, at a connection speed of 56 kbps;
- use of the „Back" button must not cause errors;
- links can use different colours, but the set of colours (active, visited, non-visited) should be the same for all the pages
- Web pages must not produce „pop-up" windows;
- all the images should be described;
- the incomplete transaction statute should be saved, and the interface should permit to recoup these;
- the interface should visualise the information transfer (declarations, etc.) between user and server.

The design process will be effected in compliance with the software systems quality standards, technological solutions and instruments (Annex 2). The requirement of *access qualities* must also be added to the above-mentioned requirements; this requirement needs formalization in offers.

3.10 Special Requirements concerning the Degree of „Openness" of the System to the e-Governance Central Portal and eGovernance Gateway

The system „e-Declarații (e-Declarations)" is foreseen to have an integrated functioning with the system e-Governance, viă the access gateway (GG- Governance Gateway). In this context, regulations and procedures of organisational and technological character are needed to ensure a complete and stable functioning of the whole system.

The e-Governance system plays a role of centralization of existing local information systems. The Internet will serve as an interconnection medium that includes approved technological solutions. For the users, the Central System will make available the following:

- interconnection with the Secured Government Intranet medium (S/MIME and TLS/SSL connections of at least 128 bits);
- interaction of public services (eGovernance Central Portal, WWW, DNS, FTP, IPv4);
- authentication services, ensuring a generalised access to information resources;
- information security and protection. in conformity with user profile;

- special formats for data exchange (XML,XSL requirements);
- management functions.

The system „e-Declarații (eDeclarations)" ensures a complete internal functioning and has a role of functional „collaboration" with the e-Governance system. The system "e-Declarații" (eDeclarations) makes available for the users the following:

- internet medium or Secured Departmental Intranet, with interconnection to the eGovernance system(S/MIME and TLS/SSL connections of at least 128 bits);
- interaction of public services (Portal e-Declarations) and interconnection with the e-Governance Portal (WWW, DNS, FTP, IPv4);
- local and centralised authentication services;
- special formats for data exchange (XML,XSL requirements);
- management functions;
- service provider public function;
- internal functions of data administration and data processing.

The degree of „openness" of the System „e-Declarations" to the integrated system e-Governance is determined by the existence of common functions within the upper list. The internal functions of data administration and data processing in one system are not included in this list. The openness of the Local system to the Central system ensures a *stable* functioning of the integrated system.

In order to ensure that the Information System „e-Declarations" is perfectly *integrated, complete* and *stable*, a delimitation between internal and public services is needed, by using efficient and secured measures. There will also be established *procedural* measures of the „openness" at the implementation stage of the system.

3.11 Normative – Legal Framework

The project solutions of the Information System "e-Declarații", its exploitation instructions and norms need the establishing of a juridical support.

The Information System „e-Declarații" will created based on the internal legal and regulatory framework of the Republic of Moldova and international treaties, to which the Republic of Moldova is a party.

For the creation, utilization and maintenance of the System in function, the stipulations of the following normative-juridical acts will be taken into account:

- The Constitution of the Republic of Moldova;
- The RM President No.1743-III of 19.03.2004, on edification of information society in the Republic of Moldova;
- Law No.780-XV of 27.12.2001 on legal acts;
- Law No.317-XV of 18.07.2003 on normative acts of the Government and other central and local public administration authorities;
- Law No.467-XV of 21.11.2003 on informatization and state information resources;
- Law No.264 of 15.07.2004 on electronic document and digital signature;
- Law No.595-XIV of 24.09.1999 on international treaties of the Republic of Moldova;
- Law No.284-XV of 22.07.2004 on electronic commerce;

- Law No.1069-XIV of 22.06.2000 on informatics;
- Law No.982-XIV of 11.05.2000 on access to information;
- International human rights treaties, to which the Republic of Moldova is a party;
- Government Decision No.255 of 09.03.2005 on National Strategy of Building the Information Society – "Electronic Moldova";
- Government Decision No. 733 of 28 June 2006 regarding eGovernance Concept;
- Government Decision No.320 of 28.03.2006 on the Regulation regarding the use of digital signature in electronic documents of public authorities;
- Government Decision No.632 of 08.06.2004 on the Policy of Edification of Information Strategy in the Republic of Moldova;
- Government Decision No.272 of 06.03.2002 on the measures regarding the creation of automatized information system "State Register of Law Units";
- Government Decision No.333 of 18.03.2002 on the approval of the concept of automatized information system "State Register of Law Units" and the Regulation regarding the State Population Register;
- Government Decision No.618 of 05.10.1993 on the approval of Rules on drafting organizational documents, and approval of Instruction Types on secretariat work in specialised central public administration bodies and local public administration bodies of the Republic of Moldova;
- Government Decision No.115 of 28.02.1996 on the approval of Instructions on secretariat work in the local public administration bodies of the Republic of Moldova;
- Technical Regulation „Software Life Cycle Processes" RT 38370656-002:2006. The Official Monitor of the Republic of Moldova No.95-97 of 23.06.2006
- internal regulations and norms of fiscal bodies activities;
- regulations on interdepartmental relationships regarding the determining the order of the implementation and the functioning of electronic document circulation; performing of secretariat work, with the usage of high performance information technologies within public authorities entities.

In the process of the System creation, implementation and exploitation the following activities and behaviours shall be regulated (from legal and normative point of view),:

- the list, volume, terms and order of effected actions;
- selection, installation and observance of exploitation conditions of informatics means;
- observance of the System implementation, exploitation and development;
- material assistance to System design, implementation and development stages.

Obligations and responsibilities assumed by the engaged parties will be stipulated in the following categories of documents with an equal normative-juridical effect:

- contracts;
- records, acts, working programs and other documents signed by the parties;
- standards, instructions, directives of the respective bodies and other documents regulating the activity of fiscal bodies;
- standards, norms and other documents regulating activities of design and implementation of informatics systems;
- project documents signed by parties, including instructions of XML schemas of fiscal reports.

3.12 Parameters for Further Exploitation of the System

The further exploitation, maintenance and development of the System will be performed in compliance with the tasks and functions mentioned in the present document, which will be established more precisely during the development and implementation of the System.

Project solutions should guarantee certain parameters of further exploitation:

- high speed transactions processing at simultaneous access to the user DB, expressed in the minimal time of reaction to query;
- simplicity of learning functioning that assumes:
  - designing of screens ensuring a maximum closeness towards real models of work;
  - designing of help files (texts);
  - documentation accessibility;
  - minimizing non-operable situations;
- exploitation security that foresees:
  - correct design of events and situations that can lead to the software and data destruction;
  - exclusion of System blocking versions;
  - insurance of functioning in accident situations.

3.13 Additional Requirements

Archive refers to the informatics system and is created with the purpose to eliminate not up-to-date data from the DB.

The periodicity of information archiving and deletion is determined by the MSFI regulations, but when these are missing – by the DB administrators.

Means of archive administration must:

- permit a reciprocal exchange of data with DB;
- ensure the access of DB administrator and the carrying out of data selection and consult procedures;
- assist in the security and regulation of the identical access to DB;

Every functionary must have an email box, with a name and alias to his position, if he has a high rank position, In the case of necessity (in case of staff changes), the alias automatically passes to another person.

4. Offer Requirements

4.1 Introduction

Title: **Information System & Portal „e-Declarații (e- Declaration)"**
Domain: Collection, storage and processing of fiscal declarations, using "online: electronic means, via Internet /Intranet.
Implementation object : Main State Fiscal Inspectorate

4.2 Offer content

The Offer will be developed in conformity with the Instructions for Offerors and will contain at least proposals for solutions for all requirements for the system mentioned in chapters 3and 4 of the present TOR respecting the normative framework.

The Offer will contain Work Plan stipulating the system development stages which will be in line with the terms established in Solicitation Documents.

The Offer shall take into consideration the interoperability requirements with main eGovernance system elements: Central eGovernance Portal and eGovernance Gateway (TOR for the elements will be included in the Solicitation Documents).

4.3 Objectives

The Information System & Portal „e-Declaratii (e-Declarations)" is destined for the collection, storage and processing of data related to fiscal declarations of physical and juridical persons in the Republic of Moldova. These responsibilities are contained in the Fiscal Code and other afferent regulations. The proposed version of informatics system observes the basic principles and includes the components of the e-Governance implementation concept.

Beneficiary: Main State Fiscal Inspectorate, Ministry of Finance. (http://www.fisc.md)

4.4 Requirements to the System

4.4.1 Functional Characteristics

B.1. Online *registration* of fiscal declarations, using the Internet medium and Internet means, through designing a Portal included in an Informatics System.

Initial conditions:

- the portal will permit the registration of 6-10 millions of fiscal declarations annually, of an approximate volume of 100 MB;
- the Offerors will design the Portal and means of adjusting for a minimum client-system reaction of 0-30s;

B.2. Configuration and *following the stream* of all categories of fiscal declarations.

B.3. *Interoperability* with the existing system of MSFI, State Treasury and other informatics systems, using editing and presentation instruments for data in XML format..

B4. Automatized creation of online *collecting procedures* of fiscal declarations, on the basis of approved declaration forms.

B.5. Different *levels of access* (differentiated levels of access at operation: completion, procession, registration, verification)

B.6. A flexible system of preventive *reporting*, corresponding to various criteria: document type, name of persons, time-term of presentation.

B.7. *Archiving.* The system of collection of fiscal declarations ***will*** effect, operatively and statutory, the archiving of data in the existing Informatics System, which will be further exploited as a basic MSFI platform.

B.8. *Searching* documents, according to various criteria: - registration number, date of document deposit, name of tax-payer, address, type of declaration, keyword, etc.

B9. Adjustment of *connection means* to the Portal, via Internet (e-Governance).

B10. Portal *specific functions*:

- ensuring of information - assistance, training, informing ;
- presence lists - contacts, reference addresses;
- options of System interaction;
- accounting and adapting of users and profiles;
- interfaces with access security and authentication means;
- content management application;
- instruments to create forms of document presentation;
- message mechanisms, routing documents to the addressee, converting them into destinations system format;
- a unitary regulation mechanism, establishing the rules of processing documents;
- working interface;
- content management application;
- a unitary structure for service development, management and maintenance;
- other functions.

4.4.2 Requirements Regarding Reliability

C1. The Offerors ***will*** design the Portal and the means of service, ensuring a functioning regime of 24hours/ 7 days a week;

C2. The Offerors will transmit the System code source, instruments for its further development, and will provide training for the Beneficiary staff.

4.4.3 Conditions of Exploitation

D1. The project ***will*** be a modular one. The ulterior extensions must not imply reorganisation of the System data and/ or significant supplementary costs, and shall not affect the System functionality and performance.

4.4.4 Technical Resources Structure and Parameters

E1. The offer ***will*** provide the use of the MSFI currently existing technical equipment, such as:

- Portal Server – server IBM OpenPower 720 with RISK processor, and the operational system SUSE Linux Server 9;
- Operational Server - server collecting and processing fiscal declarations, using server IBM OpenPower 720 with RISC processor, operating system SUSE Linux Server 9 Database Management System Informix version 10.0, licensed for processors;

E2 The offer ***will*** present recommendations concerning supplementary technical equipment.

4.4.5 Information and System Compatibility

F1. The project ***will*** include means of adjustment with the components of the Informatics System that ***exist now*** or ***will be foreseen for the future***:

- Firewall, means to prevent non-authorised access in the network;
- authentication server for network users (Gateway), with protection SMTP and detection SPAM.
- certification server and public key infrastructure (certificate X509v3, Directory Server LDAP / X.500);
- intrusion detection system to detect traffic TCP/IP;
- WEB Mail server to receive from taxpayers, or transmit them data via e-mail;
- Anti-virus server, to protect access points of systems;
- server DNS for Name Server and Resolver (LDAP v3 /ITU X.500);

F2. The offer ***will*** regard the utilization of Internet /Intranet medium in order to use Portal services. It is recommended to include e-business services and voice applications (VoIP-voice over IP, VPN – virtual private network, QoS –quality of service, and others) ***will*** be an advantage.

F3. The system will have as support one of the industrial Relational Database Management System which:

- realise the established functional structure,
- will support the interrogation standard SQL-92,
- will support transactions,
- will include the data security techniques,
- will have a licence for unlimited number of competitive connexions,
- Will have necessary performance for realization of interactive functions and will permit a big number of users to access simultaneously and competitive data base without loss of performance,
- Will have a limit of stock capacity not less than 2 TB,
- Will have a license for unlimited number of units CPU32/64,

- Will have instruments which permit the system development and interoperability with other systems under the eGovernance concept.

4.4.6 Marking up and Packaging;

The offer ***will*** include conditions according to which all the equipment and software products will be accompanied by producer brands and indices, in conformity with the legislation in force in the Republic of Moldova.

4.4.7 Transportation and Storage;

The offer ***will*** provide delivery of CIP to the MSFI location Chisinau, Moldova.

4.4.8 Special Requirements

The offer ***will*** include special measures concerning:

- installation;
- training operators;
- testing solution;
- additional maintenance services. The Offeror will ensure total system maintenance during a one-year period since the day of its putting into operation.

4.4.9 Accompanying Documents

The offer ***will*** include the delivery of a document set, necessary for a further installation, implementation and exploitation of the System.

4.4.10 Elaboration Stages

The Offeror ***will*** design the Portal and the means of adjustment to be implemented in a 5-month period from the contract date.

Stage 1 – in a 3-week term after the Contract signing - System Technical Design approval
Stage 2. - 12 weeks after the Contract signing –Experimental functionality, including the access to services through the created by Offeror Central Portal model (see TOR ANNEX VII)
Stage 3 - 20 weeks after the Contract signing – Full functionality

4.4.11 Acceptance Act

The services are considered to be delivered by the Offeror and accepted by the Beneficiary, if the work operations have been realised in strict conformity with :
- Technical Specifications;

- Law No..467-XV of 21.11.2003 „On Informatization and State Information Resources". The Official Monitor of the Republic of Moldova No.6-12 of 01.01.2004;
- Government Decision No.562 of 22.05.2006 „On Creation of State Automotized Information Systems and Information Resources". The Official Monitor of the Republic of Moldova No.79-82 of 26.05.2006;
- Law of the Republic of Moldova No.264-XV of 15.07.2004 „On Electronic Document and Digital Signature". The Official Monitor of the Republic of Moldova No.132-137 of 06.08.2004;
- Government Decision No. 733 of 28 June 2006 regarding eGovernance Concept;
- Technical Regulation „Software Life Cycle Processes" RT 38370656-002:2006. The Official Monitor of the Republic of Moldova No.95-97 of 23.06.2006.

"On-key" end of work will be documented through an Acceptance act.

Terms and Acronyms

AES	- Advanced Encryption Standard;
Blog	- Short for Web log, a blog is a Web page that serves as a publicly accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author and can be used to express the opinion regarding different problems in the society;
DB	- Database;
Covert Channels	- a covert channel is a parasitic communications channel that draws bandwidth from another channel in order to transmit information without the authorization or knowledge of the latter channel's designer, owner, or operator;
CIP	- „CARRIAGE AND INSURANCE PAID TO";
CHAP	- Challenge Handshake Authentication Protocol;
CPU	- Central Processing Unit;
Tax-Payer	- Person who pays taxes;
CTS	- Centre for Special Telecommunications;
eGovernment,	- eGovernment is the efficient delivery of government services using the Internet;
eGovernance	.-eGovernance is using the Internet to facilitate effective decision making in the community;.
DIS	- Departmental Interface Server;
DNS	- Domain Name Server;
FIPS	- Federal Information Processing Standards;
FTP	- File Transfer Protocol;
FI	- Fiscal Inspectorate;
MSFI	- Main State Fiscal Inspectorate;
IKE	- Internet Key Exchange;
ISDN	- Integrated Services Digital Network;
ISO	- International Organization for Standardization;
LAN	- Local Area Network;
LDAP	- Lightweight Directory Access Protocol;
MIME	- Multipurpose Internet Mail Extensions;
NT	- Windows NT;
OLAP	- On Line Analytical Processing;
Patch	- A patch is a small piece of software designed to update or fix problems with a computer program;
PC	- Personal Computer;
PDA	- Personal Digital Assistant;
PKCS	- Public Key Cryptography Standards;
PKI	- Public Key Infrastructure;
Portal	- Portals are sites on the World Wide Web that typically provide personalized capabilities to their visitors. They are designed to use distributed applications, different numbers and types of middleware and hardware to provide services from a number of different sources;
POP3	- Post Office Protocol version 3;
RFC	- Request For Comments;

RISC	- Reduced Instruction Set Computer;
RM	- Republic of Moldova;
RSA	- An algorithm for public-key encryption;
RSP	– State Population Register
RSUD	– State Register of Legal Entities
IS	- Informatics System;
SIS	- Information and Security Service ;
Collateral systems	- informatics systems that have similar orientation with the "e-Declarations" informatics system;
SHA	- Secure Hash Algorithm;
SHS	- Secure Hash Standard;
SMS	- A standard used to transport the messages in the mobile telephony;
S/MIME	- Secure / Multipurpose Internet Mail Extensions;
SMTP	- Simple Mail Transfer Protocol;
SOAP	- Simple Object Access Protocol;
SPAM	- The abuse of electronic messaging systems to send unsolicited, bulk messages;
Network Spoofing	- Attack type in which one person or program successfully masquerades as another by falsifying data and thereby gains an illegitimate advantage;
SQL	- Structured Query Language;
TB	- Terabyte;
TCP/IP	- Transmission Control Protocol / Internet Protocol;
TLS/SSL	Transport Layer Security/Secure Sockets Layer;
Tunnelling	A technology that enables one network to send its data via another network's connections;
UDDI	- Universal Description, Discovery, and Integration;
VoIP	- Voice over Internet Protocol;
VPN	Virtual Private Network;
WAN	- Wide Area Network;
WWW , Web	-The **World Wide Web** ("**WWW**" or simply the "**Web**") is a global, read-write information space. Text documents, images, multimedia and many other items of information, referred to as *resources*, are identified by short, unique, global identifiers called Uniform Resource Identifiers (URIs) so that each can be found, accessed and cross-referenced in the simplest possible way
Web Browser	- A software application used to locate and display Web pages;
WDSL	- Web Services Definition Language;
	- World Wide Web;
XML	- Extensible Markup Language;
XML Schema	- A description of a XML document type;
XSD	- XML Schema Definition;
XSL	- eXtensible Stylesheet Language.

Annex 1

Threats to Information Security

a) Objects of information security threats are information resources and information infrastructure;

b) Sources of information security threats can be delinquents, corrupt state functionaries as well as ill-intentioned users;

c) The basic threats to information security are:

- illegal collection and illegal utilization of the information;
- information processing technology breakdown;
- implementation in the software and hardware products of components, which carry out unforeseen, unintended functions in the documents accompanying these products;
- creation and spreading of software affecting the normal functioning of informatic systems, telecommunications information networks, information protection systems and other informatized systems;
- erasing, deterioration, radio-electronic suppressing or destruction of processing information means and systems, telecommunication systems and communication systems;
- influence of information processing and transmission automatized systems on the protection means;
- ➢ - compromise the information protection cryptographic keys and means; --------- retrieval of information through technical channels;
- illegal installation of electronic means, for the purpose of information interception, in technical devices for processing, storing and transmission of information via communication channels, or in offices of state functionaries, with the purpose of information interception ;
- erasing, deterioration, destruction or retrieval of mechanic or electronic information supports;
- interception of information in data transmission networks and communications lines, decoding of this information and imposing of false information;
- use of non-certified information technologies, information protection means, informatising means, telecommunications and communications in the creation and development of information infrastructure;
- non-authorised access to information resources from data banks and databases;
- violation of the legal restrictions on information spreading;
- attack against an insufficiently strong key / algorithm;
- traffic analysis;
- non-authorised access to workstation;
- non-authorised access to the network /network resources;
- covert channels;
- network spoofing;
- viruses;

- spam;
- tunnelling;
- Denial of service (DoS) attack – service interruption
- repudiation;

d) the information security threats affect:
- information confidentiality;
- logical and physical integrity of information;
- normal functioning of information infrastructure;

- Information security threats can be realized in the following ways:
  - non-authorised, illegal or non-sanctioned access to information resources and infrastructure;
  - physical influence on the information infrastructure components;
  - illegal information leaking through various channels;
  - bribing and/or threatening the MSFI staff.

Annex 2

Reference Standards for Informatics Systems and e-Governance.

National Institute of Standards and Technology

FIPS 140-2
Security Requirements for Cryptographic Modules
FIPS 180-2
Secure Hash Standard, August 2002
FIPS 186-2
Digital Signature Standard, February 2000
FIPS 188
Standard Security Label for Information Transfer
FIPS 196
Entity Authentication Using Public Key Cryptography
FIPS 197
Advanced Encryption Standard (AES)
SP 800-63
Electronic Authentication Guideline, Version 1.0.1

Military Standards

MIL-STD-498
Software Development and Documentation Standard, 1989
MIL-STD-810D (2)
Environmental Test Methods and Engineering Guidelines, 19 July 1983

American National Standards Institute (ANSI)

International Organization for Standardization (ISO)

International Electro-technical Commission (IEC)

ANSI/ISO/IEC TR 9294.1990
Information Technology Guidelines for the Management of Software Documentation
ISO/IEC TR 13335-4:2000
Information technology—Guidelines for the management of IT Security—Part 4: Selection of safeguards
ISO/IEC TR 13335-3:1998
Information technology—Guidelines for the management of IT Security—Part 3 Techniques for the management of IT security
ISO/IEC TR 13335-2:1997
Information technology—Guidelines for the management of IT Security—Part 2: Managing and planning IT security
ISO/IEC TR 13335-1:1996
Information technology—Guidelines for the management of IT Security—Part 1: Concepts and models for IT security
ISO 10007:1995

Quality Mgmt. Guidelines for Configuration Management
ISO 10005-1995
Quality Mgmt. Guidelines for Quality Plans
ANSI/ISO/ASQC QS9000-3-1997
QM and QA standards Part 3: Guidelines for the application of ANSI/ISO/ASQC Q9000-1994 to the Development, Supply, Installation, and Maintenance of Computer Software

Electronic Industries Alliance Standards

MB2, MB5, MB9
Maintainability Bulletins
EIA 157
Quality Bulletin
EIA QB2-QB5
Quality Bulletins
EIA RB9
Failure Mode and Effect Analysis, Revision 71
EIA SEB1—SEB4
Safety Engineering Bulletins
RS-232-C
Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange
RS-366-A
Interface Between Data Terminal Equipment and Automatic Calling Equipment for Data Communication
RS-404
Standard for Start-Stop Signal Quality between Data Terminal Equipment and Non-synchronous Data Communication Equipment
NISTIR 4909
Software Quality Assurance: Documentation and Reviews

National Institute of Standards and Technology

Institute of Electrical and Electronics Engineers

610.12-1990
IEEE Standard Glossary of Software Engineering Terminology
730-1998
IEEE Standard for Software Quality Assurance Plans
828-1998
IEEE Standard for Software Configuration Management Plans
829-1998
IEEE Standard for Software Test Documentation
830-1998
IEEE Recommended Practice for Software Requirements Specifications

Military Standards

MIL-STD-498
Software Development and Documentation, 27 May 1998

American National Standards Institute (ANSI)

International Organization for Standardization (ISO)

International Electro-technical Commission (IEC)

ANSI/ISO/IEC TR 10176.1998
Information Technology Guidelines for the Preparation of Programming Language Standards

ANSI/ISO/IEC 6592.2000
Information Technology Guidelines for the Documentation of Computer Based Application Systems
ANSI/ISO/ASQC Q9000-3-1997
Quality management and quality assurance standards Part 3: Guidelines for the application of ANSI/IAO/ASQC Q9001-1994 to the Development, supply, installation and maintenance of computer software
ANSI/ISO/ASQC Q9000-1-1994
Quality Management and Quality Assurance Standards—Guidelines for Selection and Use
ANSI/ISO/ASQC Q10007-1995
Quality Management Guidelines for Configuration Management
ANSI X9.31-1998
Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry, 1998
ANSI X9.62-1998
Public Key Cryptography for Financial Services Industry: The Elliptic Curve Digital Signature Algorithm, 1998
ISO/IEC 9594-8:2001
ITU-T Recommendation X.509 (2000), Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

National Institute of Standards and Technology

FIPS 102
Guideline for Computer Security Certification and Accreditation
FIPS 112
Password Usage (3)
FIPS 113
Computer Data Authentication

Institute of Electrical and Electronics Engineers

488-1987
IEEE Standard Digital Interface for Programmable Instrumentation
796-1983
IEEE Standard Microcomputer System Bus IEEE/ANSI Software Engineering Standards
750.1-1995
IEEE Guide for Software Quality Assurance Planning
1008-1987
IEEE Standard for Software Unit Testing
1016-1998
IEEE Recommended Practice for Software Design Descriptions
1012-1998
IEEE Guide for Software Verification and Validation Plans

Other References

Designing for the Color-Challenged: A Challenge, by Thomas G. Wolfmaier (March 1999); http://www.sandia.gov/itg/newsletter/mar99/accessibility_color_challenged.html;
Effective Color Contrast: Designing for People with Partial Sight and Color Deficiencies, by Aries Arditi, Ph.D; http://www.lighthouse.org/color_contrast.htm
Electronic Markup Language (EML), Version 4.0, (Committee Draft) Organization for the Advancement of Structured Information Standards (OASIS), January 24, 2005
RSA Laboratories Technical Note, Public Key Cryptographic Standard (PKCS) #7: Cryptographic Message Syntax Standard, November 1, 1993

RSA Laboratories Technical Note, Extensions and Revisions to PKCS #7, May 13, 1997
The Americans with Disabilities Act Accessibility Guidelines (ADAAG 2202), Access Board;
http://www.access-board.gov/adaag/html/adaag.htm

Annex 3

List of Fiscal Declarations Forms

Value Added Tax
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/taxa_val_adaugata.ascx
Tax on Property
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/improp.ascx
Income Tax
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/impozit_pe%20venit.ascx
Private Tax
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/impozit_privat.ascx
Natural Resources Tax
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/impoz_res_nat.ascx
Road Fund Tax
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/taxa_fond_rutier.ascx
Local Taxes
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/taxe_locale.ascx
Tax on Dividends
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/doc/dividende/dividende.ascx
Excise Tax
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/accize.ascx
Medical Assistance Property Taxes
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/CNAM.ascx
Social Assistance Installments
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/CNAM.ascx
State Markup on Alcoholic Products
http://www.fisc.md/INDEX_main.aspx?source=doc/ro/declaratii/msta.ascx

Annex IV

PROPOSAL SUBMISSION FORM

Dear Sir / Madam,

Having examined the Solicitation Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to provide Professional Consulting services (profession/activity for
Project/programme/office) for the sum as may be ascertained in accordance with the Price Schedule attached herewith and made part of this Proposal.

We undertake, if our Proposal is accepted, to commence and complete delivery of all services specified in the contract within the time frame stipulated.

We agree to abide by this Proposal for a period of 120 days from the date fixed for opening of
Proposals in the Invitation for Proposal, and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

We understand that you are not bound to accept any Proposal you may receive.

Dated this day /month of year

F. Signature

(In the capacity of)

Duly authorised to sign Proposal for and on behalf of

Annex V

PRICE SCHEDULE

The Contractor is asked to prepare the Price Schedule as a separate envelope from the rest of the RFP response as indicated in Section D paragraph 14 (b) of the Instruction to Offerors.

All prices/rates quoted must be exclusive of all taxes, since the UNDP is exempt from taxes as detailed in Section II, Clause 18. '

The Price Schedule must provide a detailed cost breakdown. Provide separate figures for each functional grouping or category.

Estimates for cost-reimbursable items, if any, such as travel, and out of pocket expenses should be listed separately.

In case of an equipment component to the service provided, the Price Schedule should include figures for both purchase and lease/rent options. The UNDP reserves the option to either lease/rent or purchase outright the equipment through the Contractor.

The format shown on the following pages should be used in preparing the price schedule. The format includes specific expenditures, which may or may not be required or applicable but are indicated to serve as examples.

In addition to the hard copy, if possible please also provide the information on diskette (IBM compatible).

Price Schedule:

Request for Proposals for Services

Description of Activity/Item		**Number of Staff**	**G.** Monthly Rate	**Estimated Amount**
1.	**Remuneration**			
1.1	Services in Home office			
1.2	Services in Field			
2.	**Out of Pocket Expenses**			
2.1	Travel			
2.2	Per Diem Allowances			
2.3	Communications			
2.4	Reproduction and Reports			
2.5	Equipment and other items			